Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Amended) A system for selectively accepting an electronic message having ~~sent from~~ a sender address and sent from ~~through~~ a remote host ~~over a connection~~ to a recipient, the system comprising:

a ~~dialup~~ client filter determining whether the ~~connection~~ remote host is a client computer~~a dialup connection~~;

a relay filter determining whether the remote host is an open relay;

an address verification filter determining ~~a user filter verifying~~ whether the sender address exists~~of the electronic message is authorized~~; and,

an ~~recipient whitelist~~ access database including a list of ~~acceptable~~ sender addresses for at least one recipient, wherein said system accepts the electronic message if said ~~dialup~~ client filter determines that the ~~connection~~ remote host is a client computer~~a dialup connection~~, or said relay filter determines that the remote host is an open relay, or said ~~user~~ address verification filter determines that the sender ~~is not authorized~~address does not exist, ~~then~~ and said system determines ~~whether~~ that the sender address is ~~in said recipient whitelist~~ permitted by said access database.

2. (Amended) The system of claim 1, wherein the sender ~~is contained in~~ address is permitted by said ~~recipient whitelist~~ access database if ~~a MAIL From address of the sender matches a substring stored in~~ said ~~recipient whitelist~~ access database contains the sender address.

3. (Original) The system of claim 1, wherein the list of acceptable sender addresses includes a null set of sender addresses.

4. (Amended) The system of claim 1, further comprising a quarantine database, wherein if said ~~user~~ address verification filter determines that the sender address does not exist~~is not authorized~~, the sender address is not ~~in~~ permitted by said ~~recipient whitelist~~ access database, and the ~~user~~ address verification filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

5. (Amended) The system of claim 1, further comprising a quarantine database, wherein if said ~~user~~ address verification filter determines that the sender ~~is not authorized~~address does not exist, the sender address is not in said ~~recipient whitelist~~ access database, and the ~~user filter~~ address verification filter is not flagged for quarantining, then the message is rejected for that recipient.

6. (Amended) The system of claim 1, further comprising a quarantine database, wherein if said ~~dialup~~ client filter determines that the ~~connection~~ remote host is ~~a dialup connection~~a client computer, the sender address is not permitted by ~~in~~ said ~~recipient whitelist~~ access database, and

the ~~dialup~~ client filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

7. (Amended) The system of claim 1, further comprising a quarantine database, wherein if said ~~dialup~~ client filter determines that the remote host ~~connection~~ is ~~a dialup~~a client computer, the sender address is not permitted by ~~in~~ said ~~recipient whitelist~~ access database, and the ~~dialup~~ client filter is not flagged for quarantining, then the message is rejected for that recipient.

8. (Amended) The system of claim 1, further comprising a quarantine database, wherein if said relay filter determines that the remote host is an open relay, the sender address is not permitted by ~~in~~ said ~~recipient whitelist~~ access database, and the relay filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database

9. (Amended) The system of claim 1, further comprising a quarantine database, wherein if said relay filter determines that the remote host is an open relay, the sender address is not permitted by ~~in~~ said ~~recipient whitelist~~ access database, and the relay filter is not flagged for quarantining, then the message is rejected for that recipient.

10. (Amended) A system for selectively accepting an electronic message having ~~sent from~~ a sender address and sent from ~~through~~ a remote host to a recipient, the system comprising:

a ~~dialup~~ client filter determining whether the ~~connection~~ remote host is ~~a dialup connection~~a client computer;

a relay filter determining whether the remote host is an open relay;

an ~~user~~ address verification filter determining ~~verifying~~ whether the sender address of the electronic message ~~is authorized~~exists; and,

a quarantine database, wherein if one or more of said ~~dialup~~ client filter, relay filter or ~~user~~ address verification filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database when said flagged ~~dialup~~ client filter determines that the ~~connection~~ remote host is ~~a dialup connection~~a client computer, said flagged relay filter determines that the remote host is an open relay, or said flagged ~~user~~ address verification filter determines that the sender ~~is not authorized~~address does not exist.

11. (Amended) The system of claim 10, wherein a user with a web browser~~at the local MTA~~ can selectively forward~~retrieve~~ the quarantined message addressed to that user.

12. (Original) The system of claim 11, further comprising a blacklist database having a list of blacklisted network addresses, wherein when the quarantined message is retrieved, ~~a~~the blacklisted network address for that remote host is removed from the said blacklist database.

13. (Amended) The system of claim 10, wherein if one or more of said ~~dialup~~ client filter, relay filter or ~~user~~ address verification filter are not flagged for quarantining, then the message is

rejected for that recipient when said unflagged ~~dialup~~ client filter determines that the ~~connection~~ remote host is ~~a dialup connection~~a client computer, said unflagged relay filter determines that the remote host is an open relay, or said unflagged ~~user~~ address verification filter determines that the sender ~~is not authorized~~address does not exist.

14. (Amended) An article of manufacture for selectively accepting an electronic message ~~sent from~~ having a sender address and sent from ~~through~~ a remote host to a recipient, the article of manufacture comprising a computer-readable medium having stored thereon instructions which, when performed by a processor, cause the processor to execute the steps comprising the steps of:

determining at least one of whether the ~~connection is a dialup connection~~remote host is a client computer, the remote host is an open relay or the sender address exists~~is authorized~~; and,

determining whether ~~a~~ the sender address of the electronic message is matched in an ~~recipient whitelist~~ access database in response to determining that the ~~connection was established by~~ remote host is a client computer~~a dialup connection~~, the remote host is an open relay or the sender address does not exist~~is not authorized~~.

15. (Amended) The article of manufacture of claim 14, wherein the sender address is ~~identified in~~ permitted by said access ~~the recipient whitelist~~ database if ~~a MAIL From address of the sender matches a substring stored~~ ~~in the~~ said ~~recipient whitelist~~ access database contains the sender address.

16. (Amended) The article of manufacture of claim 14, further comprising flagging at least one of the determining whether the ~~connection is a dialup~~remote host is a client computer, the remote host is an open relay or the sender address exists~~is authorized~~ and quarantining any message when the at least one flagged determining determines that the ~~connection is a dialup~~remote host is a client computer, the remote host is an open relay or the sender address does~~is~~ not ~~authorized~~exist.

17. (Amended) A method for selectively accepting an electronic message having a sender address and transferred ~~over a connection~~ from ~~a sender through~~ a remote host to a recipient, the method comprising:

determining at least one of whether the ~~connection is a dialup connection~~remote host is a client computer, the remote host is an open relay or the sender address does not exists~~is authorized~~; and,

determining whether ~~a~~ the sender address of the electronic message is identified in an ~~recipient whitelist~~ access database in response to determining that the ~~connection was established by~~ remote host is a client computer~~dialup connection~~, the remote host is an open relay or the sender address does not exist~~is not authorized~~.

18. (Amended) The ~~system~~ method of claim 17, further comprising adding the remote host to a blacklist database if the electronic message is from a client computer or the remote host is an

open relay or the sender address does not exist, and the sender address is not matched in said ~~any recipient whitelist~~ access database.

19. (Amended) The ~~article of manufacture~~ method of claim 17, wherein the sender address is ~~identified in~~ permitted by said ~~the recipient whitelist~~ access database if ~~a MAIL From address of the sender matches a substring stored in the~~ said ~~recipient whitelist~~ access database contains the sender address.

20. (Original) A method for selectively accepting an electronic message comprising providing at least one filter that determines whether the electronic message is undesirable, flagging at least one filter for quarantining, and quarantining the electronic message for any flagged filter if that filter determines that the electronic message is undesirable.

21. (Amended) The method of claim 20, wherein a system administrator or ~~the~~ a message recipient can selectively retrieve the quarantined electronic message.

22. The method of claim 21, further comprising storing a list of blacklisted network addresses, and removing a blacklisted network address for the remote host when the quarantined message is retrieved.

23. (Amended) A system for selectively accepting an electronic message having a sender address and sent from a ~~sender through a~~ remote host ~~over a connection~~ to a recipient, the system comprising a ~~dialup~~ client filter determining whether the ~~connection is a dialup connection~~ remote host is a client computer and an access ~~recipient whitelist~~ database including a list of ~~acceptable~~ sender addresses, wherein if said ~~dialup~~ client filter determines that the ~~connection is a dialup connection~~remote host is a client computer, then said system accepts the message for that recipient if the sender address is ~~in~~ permitted by said ~~recipient whitelist~~ access database.

24. (Amended) The system of claim 23, further comprising a blacklist database, wherein the remote host is added to the blacklist database if the remote host is determined to be a client computer and the sender address is not matched in ~~any recipient whitelist~~ said access database.

25. (Amended) The system of claim 23, wherein said system rejects the message for that recipient if said ~~dialup~~ client filter determines that the ~~connection is a dialup connection~~ remote host is a client computer and the sender address is not in said ~~recipient whitelist~~ access database.

26. (Amended) The system of claim 23, further comprising a quarantine database, wherein if said ~~dialup~~ client filter determines that the ~~connection is a dialup connection~~remote host is a client computer, the sender address is not in said ~~recipient whitelist~~ access database, and the ~~dialup~~ client filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

27. (Amended) A system for selectively accepting an electronic message sent from a sender address through a remote host to a recipient, the system comprising a relay filter determining whether the remote host is an open relay and an ~~recipient whitelist~~ access database including a list of ~~acceptable~~ sender addresses, wherein if said relay filter determines that the remote host is an open relay, then said system accepts the message for that recipient if the sender address is in said ~~recipient whitelist~~ access database.

28. (Amended) The system of claim 27, further comprising a blacklist database, wherein the remote host is added to the blacklist database if the sender address is not matched in ~~any recipient whitelist~~ said access database.

29. (Amended) The system of claim 27, wherein said system rejects the message for that recipient if said relay filter determines that the remote host is an open relay and the sender address is not in said ~~recipient whitelist~~ access database.

30. (Amended) The system of claim 27, further comprising a quarantine database, wherein if said relay filter determines that remote host is an open relay, the sender address is not in said ~~recipient whitelist~~ access database, and the relay filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

31. (Amended) A system for selectively accepting an electronic message having ~~sent from~~ a sender address and sent from ~~through~~ a remote host to a recipient, the system comprising an address verification ~~user~~ filter ~~determining~~verifying whether the sender address exists~~of the electronic message is authorized~~; and an access ~~recipient whitelist~~ database including a list of ~~acceptable~~ sender addresses, wherein if said ~~user~~ address verification filter determines that the sender ~~is not authorized~~address does not exist, then said system accepts the message for that recipient if the sender address is in said ~~recipient whitelist~~ access database.

32. (Amended) The system of claim 31, further comprising a blacklist database, wherein the remote host is added to the blacklist database if the sender address is not matched in ~~any~~ said ~~recipient whitelist~~ access database.

33. (Amended) The system of claim 31, wherein said system rejects the message for that recipient if said ~~user~~ address verification filter determines that the ~~user is not authorized~~sender address does not exist, and the sender address is not in said ~~recipient whitelist~~ access database.

34. (Amended) The system of claim 31, further comprising a quarantine database, wherein if said ~~user~~ address verification filter determines that the sender ~~is not authorized~~address does not exist, the sender address is not in said ~~recipient whitelist~~ access database, and the ~~user~~ address verification filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

35. (Amended) A system for selectively accepting an electronic message having ~~sent from~~ a sender address and sent from ~~through~~ a remote host ~~over a connection~~ to a recipient, the system comprising a ~~dialup~~ client filter determining whether the ~~connection is a dialup connection~~ remote host is a client computer and a quarantine database, wherein if said ~~dialup~~ client filter determines that ~~the connection is a dialup connection~~ the remote host is a client computer and the ~~dialup~~ client filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

36. (Amended) The system of claim 35, wherein said system rejects the message for that recipient if said ~~dialup~~ client filter determines that the ~~connection is a dialup connection~~ remote host is a client computer and the ~~dialup~~ client filter is not flagged for quarantining.

37. (Original) The system of claim 35, further comprising a blacklist database having a list of blacklisted network addresses, wherein when the quarantined message is retrieved, a blacklisted network address for that remote host is removed from said blacklist database.

38. (Amended) A system for selectively accepting an electronic message ~~sent from~~ having a sender address and sent from ~~through~~ a remote host to a recipient, the system comprising a relay filter determining whether the remote host is an open relay and a quarantine database, wherein if said relay filter determines that remote host is an open relay and the relay filter is

flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

39. (Original) The system of claim 38, wherein said system rejects the message for that recipient if said relay filter determines the remote host is an open relay and the relay filter is not flagged for quarantining.

40. (Original) The system of claim 38, further comprising a blacklist database having a list of blacklisted network addresses, wherein when the quarantined message is retrieved, a blacklisted network address for that remote host is removed from said blacklist database.

41. (Amended) A system for selectively accepting an electronic message having ~~sent from~~ a sender address and sent from ~~through~~ a remote host to a recipient, the system comprising an address verification ~~user~~ filter ~~verifying~~ determining whether the sender address exists~~of the electronic message is authorized~~, and a quarantine database, wherein if said ~~user~~ address verification filter determines that the sender address does not exist~~is not authorized~~ and the ~~user~~ address verification filter is flagged for quarantining, then the message is quarantined for that recipient in said quarantine database.

42. (Amended) The system of claim 41, wherein said system rejects the message for that recipient if said ~~user~~ address verification filter determines that the user is not authorized and the ~~user~~ address verification filter is not flagged for quarantining.

43. (Original) The system of claim 41, further comprising a blacklist database having a list of blacklisted network addresses, wherein when the quarantined message is retrieved, a blacklisted network address for that remote host is removed from said blacklist database.

44. (New) A method for selectively accepting an electronic message having a sender address and transferred from a remote host to a recipient, the method comprising determining whether the sender address exists.

45. (New) The method of claim 44, wherein the step of determining whether the sender address exists determines the quality of an initial affirmative response by issuing a test message having an address that is believed to not exist, and accepting the electronic message if the test message is rejected.

46. (New) A method for selectively accepting an electronic message having a potentially forged sender address, the potentially forged sender address having a sender domain name, from a remote host having a domain name to one or more recipients, the method comprising determining if the remote host is in the hierarchical domain of the sender address, and accepting the electronic message if the remote host is in the domain of the sender address.

47. (New) A method for selectively accepting an electronic message transferred from a remote host to one or more users, the method comprising sending protocol transactions to the remote host and monitoring the remote host response to determine whether the remote host will accept transactions that might be used to forward mail from an unknown origin by the remote host, rejecting the electronic message if the remote host accepts the transaction.

48. (New) A method for verifying an e-mail address having a sending domain, the method comprising sending a test message specifying the e-mail address to an authorized mailhost for the sending domain, accepting the e-mail address if the authorized mailhost accepts the test message, and rejecting the e-mail address if the authorized mailhost does not accept the test message.

49. (New) The method of claim 48, where the authorized mailhost is a mail exchanger host for the domain of the e-mail address..

50. (New) The method of claim 48, where the authorized mailhost is the host with the sending domain of the e-mail address.

51. (New) A method for verifying an e-mail address having a sending domain, the method comprising sending a first test message specifying the e-mail address to an authorized mailhost for the sending domain, marking the e-mail address as invalid if the authorized mailhost does not accept the first test message, sending a second test message specifying an e-mail address that is believed to not exist to the authorized mailhost if the authorized mailhost accepts the first test message, marking the e-mail address as valid if the authorized mailhost accepts the first test message and rejects the second test method, and marking the e-mail address as indeterminate if the authorized mailhost accepts both the first and second test messages.